IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik

Yudhi Arta[1], Abdul Syukur[2], Roni Kharisma[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
[1]yudhiarta@eng.uir.ac.id, [2]abdulsyukur@eng.uir.ac.id, [3]roni100194@gmail.com

Abstract

Computer network security is part of a system that is critical to maintaining the validity and integrity of data and ensuring the availability of services for its users. Current network intrusion detection systems are generally able to detect attacks but are unable to take further action. But on the one hand humans are very dependent with the information system. This is what causes the statistics of network security incidents continue to increase sharply from year to year. This is due to the very poor people's concern for the network security system. Therefore a system that can help network administrator to be used as monitor network traffic with Intrusion Prevention System (IPS) which is a combination of facility blocking capabilities of Firewall.

Keywords : *firewall, Intrusion Prevention System, router mikrotik.*

Abstrak

Keamanan jaringan komputer merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan. Maka dari itu dibutuhkan sebuah sistem yang dapat membantu network administrator untuk digunakan sebagai monitor trafik jaringan dengan *Intrusion Prevention System* (IPS) yang merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall.*

Kata kunci: *firewall, Intrusion Prevention System, router mikrotik.*

1. PENDAHULUAN

Keamanan jaringan komputer merupakan bagian dari sebuah sistem yang sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mampu mengambil tindakan lebih lanjut.[1][2][3][4]

Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat *free* dan ada pula yang dikomersilkan. Kemudian dari sisi *software* pendukung pun sudah banyak *tool-tool* yang bersifat *free* yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan *intruder* dan *attacker*.

2. METODE PENELITIAN

Metode penelitian adalah cara dan langkah-langkah yang digunakan dalam melakukan penelitian. Pada penelitian dalam proses pengkajian data mining ini, cara dan langkah-langkah yang digunakan antara lain : Pengumpulan Data, Konsep Teori, dan Perancangan Sistem. Uraian metode penelitian yang digunakan dapat diuraikan sebagai berikut :

2.1 Pengumpulan Data

Dalam proses pengumpulan data, untuk mendapatkan data yang benar dan meyakinkan agar hasil yang dicapai tidak menyimpang dari tujuan yang telah diterapkan sebelumnya, penulis melakukan langkah langkah penelitian sebagai berikut :

1. Analisis
   Metode ini gunanya untuk menganalisa sebuah rancangan yang telah dibangun, menganalisa proses dari penyerangan yang terjadi hingga mendapat pemeritahuan dalam bentuk *e-mail*.
2. Perancangan
   Tahap ini akan meneterjemahkan spesifikasi kebutuhan yang telah didapat pada tahap analisis kedalam bentuk arsitektural perangkat lunak untuk di implementasikan kepada aplikasi yang dibuat
3. Pengujian
   Dalam tahap pengujian dilakukan dengan menggunakan aplikasi untuk mendapatkan hasil pengujian yang sedang berjalan.
4. Dokumentasi
   Pada proses dokumentasi, penulis juga melakukan studi pustaka, membaca dan mempelajari dokumen-dokumen, buku-buku acuan, serta sumber lainnya yang berkaitan dengan penelitian untuk dijadikan referensi.

2.2 Dasar Teori

Teori yang yang digunakan pada penelitian ini dapat diuraikan sebagai berikut :

2.2.1 Router

Router merupakan sebuah *device* atau alat yang dapat menghubungkan dua atau lebih jaringan komputer yang berbeda. Secara umum *router* adalah suatu alat pada jaringan komputer yang bekerja di *networklayer* pada lapisan *OSI*. Dalam *Router* ini terdapat *routing table* yaitu table yang berisi alamat-alamat jaringan yang dibutuhkan untuk memenuhi tujuan dari paket-paket data yang akan dilewatkan pada suatu jaringan tersebut.

Untuk membuat suatu *router*, kita dapat memanfaatkan suatu jenis *operating system* seperti *operating systemWindows*, *Unix*, *Linux* atau jenis *operaring* sistem lain pada komputer *PC* kita dengan hanya menambahkan 2 buah *Network Interface*

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Card(NIC). Jika komputer kita sudah memiliki *NIC* misalnya *PC* yang sudah *onboard*, maka kita cukup menambahkan 1 buah *NIC* lagi. Dengan bantuan implementasi dari router ini kita bisa membuat suatu jaringan *LAN* dengan kelas yang berbeda-beda, misalnya kelas B dan Kelas C ataupun kelas lainnya.

2.2.2 Firewall

firewall adalah alat yang digunakan untuk mencegah orang luar untuk memperoleh akses ke suatu jaringan. *Firewall* pada umumnya merupakan suatu kombinasi dari perangkat lunak dan perangkat keras. Firewalls biasanya menerapkan pengeluaran rencana atau perintah untuk menyortir alamat yang tak dikehendaki dan diinginkan.[5]

Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi. Hal ini dapat dibagi menjadi dua bagian:

1. Apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibitted*)
2. Apa-apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*)

Firewall bekerja dengan mengamati packet *IP* (*Internet Protocol*) yang melewatinya. Berdasarkan konligurasi dari firewall maka akses dapat diatur berdasarkan *IP address, port,* dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall*. Untuk memahami bagaimana *firewalls* bekerja, Pengesahan pertama, paling sederhana memeriksa prosedur penggunaan *IP* alamat sebagai suatu index. *IP* alamat index identifikasi universal pad *internet* . baik alamat statis maupun alamat yang dinamis.

IP alamat statis adalah alamat yang permanen yang merupakan alamat dari suatu mesin yang selalu dihubungkan ke *Internet*. Ada banyak kelas dari alamat *IP* statis. Satu kelas dapat ditemukan dengan *query,* kelas ini mesin tertinggi yang terhubung dengan jaringan, seperti domain dari *server, Web server*, dan root-level mesin. Yang sudah terdaftar sebagai *hostnames* pada *databaseInterNIC*. Kelas yang lain dari alamat *IP* statis adalah alamat yang ditugaskan kedua dan ketiga dari level mesin di dalam jaringan yang dikuasai oleh domain yang disebut *server, root server*, *Web server*, dan lainnya.

2.2.3 Protocol

protocol merupakan aturan-aturan dan prosedur untuk melakukan komunikasi. Ketika beberapa komputer dalam sebuah jaringan hendak melakukan komunikasi dengan komputer lain, aturan-aturan atau prosedur komunikasi harus dilakukan terlebih dahulu. Atuan-aturan tersebut dikenal dengan istilah *protocol.*

Beberapa hal yang perlu kita pahami tentang *protocol* dalam sebuah lingkungan jaringan komputer adalah sebagai berikut :

1. Dalam sistem jaringan komputer terdapat beberapa jenis *protocol,* masing-masing memiliki tujuan dan tugas yang berbeda. Setiap *protocol* memiliki kelebihan dan kekurangan.
2. Beberapa *protocol* dapat saling bekerjasama. Hal ini dikenal dengan istilah *protocol stack* atau *protocol suite.*

2.2.4 Web Server

web server adalah software yang menjadi tulang belakang dari *world wide web* (www) yang pertama kali tercipta sekitar tahun 1980an**.** *Web server* menunggu permintaan dari *client* yang menggunakan *browser* seperti *Netscape Navigator, Internet Explorer, Mozilla Firefox*, dan program browser lainnya. Jika ada permintaan dari browser, maka *web server* akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke *browser*.[6]

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Data ini mempunyai format yang standar, disebut dengan format *SGML* (S*tandar General Markup Language*). Data yang berupa format ini kemudian akan ditampilkan oleh *browser* sesuai dengan kemampuan *browser* tersebut. Contohnya, bila data yang dikirim berupa gambar, *browser* yang hanya mampu menampilkan teks (misalnya *lynx*) tidak akan mampu menampilkan gambar tersebut, dan jika ada akan menampilkan alternatifnya saja.

Web server, untuk berkomunikasi dengan *client*-nya (*web browser*) mempunyai protokol sendiri, yaitu *HTTP* (*hypertext transfer protocol*). Dengan protokol ini, komunikasi antar *web server* dengan *client*-nya dapat saling dimengerti dan lebih mudah. Seperti telah dijelaskan diatas, format data pada *world wide web* adalah *SGML*. Tapi para pengguna internet saat ini lebih banyak menggunakan format *HTML* (*hypertext markup language*) karena penggunaannya lebih sederhana dan mudah dipelajari.

Standarisasi *web server* dalam penerapan penggunaannya antara lain dikeluarkan oleh *W3C* (*World Wide Web Consortium*), *IETF* (*Internet Engineering Task Force*), dan beberapa organisasi lainnya. Sampai saat ini, sudah lebih dari 110 spesifikasi yang dirilis oleh W3C (*W3C Recommendations*). [7]

Contoh standarisasi *web server* antara lain :

1. Spesifikasi *HTML, CSS, DOM* dan *XHTML (W3C)*
2. Spesifikasi *Javascript (ECMA)*
3. *URL, HTTP (IETF)* dalam bentuk dokumen *RFC*

2 2.5 Snort

Snort merupakan salah satu contoh program *Network-based Intrusion Detection System*, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. *Snort* bersifat *open source* dengan lisensi *GNU General Purpose License* sehingga software ini dapat dipergunakan untuk mengamankan sistem *server* tanpa harus membayar biaya lisensi.[8][9][10]

Suatu sistem *IDS* harus bersifat lintas platform, mempunyai sistem *footprinting* yang ringan, dan mudah dikonfigurasi oleh administrator sebuah sistem yang membutuhkan implementasi dari solusi kemananan dalam waktu yang singkat. Implementasi tersebut dapat berupa seperangkat *software* yang dapat diasosiasikan dalam melakukan aksi untuk merespon sistuasi keamanan tertentu. Selain itu. sebuah sistem *IDS* juga harus *powerfull* dan cukup fleksibel untuk digunakan sebagai bagian permanen dari suatu sistem jaringan.

Snort memenuhi kriteria tersebut, yaitu dapat dikonfigurasi dan dibiarkan berjalan untuk periode yang lama tanpa meminta pengawasan atau perawatan bersifat administratif sebagai bagian dari sistem keamanan terpadu sebuah infrastruktur jaringan. *Snort* iuga dapat berjalan pada semua *platform* sistem operasi di mana *libpcap* dapat berjalan. Sampai saat ini, Snort telah teruji dapat berjalan pada sistem operasi *RedHat Linux, Debian Linux, MkLinux, HP-UX, Solaris (x86 dan Sparc), x86 Free/Net/OpenBSD, Windows* dan *MacOS X.*

2 2.6 Intrusion Prevention System

Intrusion Prevention System (*IPS*) adalah pendekatan yang sering digunakan *system* keamanan komputer, *IPS* mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (*IDS*) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket semua paket dan serta mengenali paket dengan sensor, disaat *attack* telah teridentifikasi, *IPS* akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Jadi *IPS* bertindak seperti layaknya *firewall* yang akan melakukan

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

allow dan *block* yang dikombinasikan seperti *IDS* yang dapat mendeteksi paket secara detail. *IPS* menggunakan *signatures* untuk mendeteksi di aktifitas trafik di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound- outbound*) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal.[11][12]

2 2.7 OSI (Open System Interconnection) Layer

1. *Phisycal Layer*
   lapisan ini bertanggung jawab untuk mengaktifkan dan mengatur physical interface jaringan komputer. Pada lapisan ini, hubungan antara *interface-interface* dari perangkat keras diatur seperti hubungan antara *DTE* dan *DCE*. Interface yang didefenisikan pada lapisan ini antara lain: 10BaseT, 100BaseTX, V35, X.21 dan *High Speed S erial Interface (HSSI).*[13][14]
2. *Data Link Layer*
   Lapisan ini mengatur topologi jaringan, *error notification* dan *flow control*. Tugas utama *datalink layer* adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi.
   Sebelum diteruskan ke *network layer*, data *link layer* melaksanakan tugas ini dengan memungkinkan pengirim memecah-mecah data *input* menjadi sejumlah *data frame* (biasanya berjumlah ratusan atau ribuan byte). Kemudian *data link layer* mentransmisikan *frame* tersebut secara berurutan, dan memproses *acknowledgementframe* yang dikirim kembali oleh penerima.[15]
3. *Network Layer*
   Network layer berfungsi untuk pengendalian operasi subnet denganmeneruskan paket-paket dari satu node ke node lain dalam jaringan. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya.
4. *Transport Layer*
   Fungsi dasar *transport layer* adalah menerima data dari *session layer*, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke *network layer*, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi *layer-layer* bagian atas dari perubahan teknologi hardware yang tidak dapat dihindari.
5. *Session Layer*
   Session layer mengijinkan para pengguna untuk menetapkan *session* dengan pengguna lainnya. Layer ini membuka, mengatur dan menutup suatu session antara aplikasi-aplikasi.
6. *Presentation Layer*
   Presentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Selain memberikan sarana-sarana pelayanan untuk konversi, format dan enkripsi data, presentation layer juga bekerja dengan file berformat *ASCII, EBCDIC, JPEG, MPEG, TIFF, PICT, MIDI,* dan *Quick Time.*

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

7. *Application Layer*

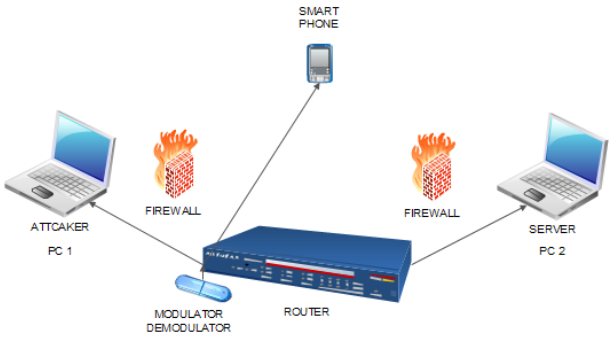
   Lapisan ini bertugas memberikan sarana pelayanan langsung ke *user*, yang berupa aplikasi-aplikasi dan mengadakan komunikasi dari program ke program. Jika kita mencari suatu *file* dari *file server* untuk digunakan sebagai aplikasi pengolah kata, maka proses ini bekerja melalui layer ini. Demikian pula jika kita mengirimkan *e-mail, browse* ke *internet, chatting,* membuka *telnet session,* atau menjalankan *FTP*, maka semua proses tersebut dilaksanakan di layer ini.

2 2.8 Flowchart

Flowchart adalah penggambaran secara grafik dari langkah-langkah danurut-urutan prosedur dari suatu program. *Flowchart* menolong analis danprogrammer untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalampengoperasian.*Flowchart* biasanya mempermudah penyelesaian suatu masalah khususnya masalah yang perlu dipelajari dan dievaluasi lebih lanjut.

2.3 Perancangan Program

Pada implemetasi jaringan dibawah ini terdapat 2 *PC*, *PC* 1 berfungsi sebagai *attacker* dengan system operasi *windows* 7 *ultimate*. *PC* 2 berfungsi sebagai *server* dengan system operasi *windows* 7 *ultimate* dan *winbox*. Terdapat juga 1 *router*, 1 *modem* dan 1 *smart phone* untuk pemberitahuan serangan yang terjadi.



Gambar 1. Perancangan *Intrusion Prevention system*

Dari implementasi diatas dapat dilihat bahwa attacker akan mencoba menyerang ip server yang telah disediakan sebelumnya dengan memasukan username dan password yang tidak dikatahui oleh attacker kemudian server akan merespon serangan yang terjadi dan menyampaikan informasi ke smartphone dalam bentuk electronic mail (email). Tujuan pemberitahuan informasi melalui email adalah untuk mengantisipasi administrator yang tidak bisa selalu berada di depan server dimana modem yang tersedia telah disetting sebagai sumber internet yang dihubungkan ke router. Server juga akan mendapat informasi serangan yang terjadi karena sudah memliki layanan log sebagai pendeteksi serangan untuk memudahkan administrator yang berada didepan server.

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Setelah Menerapkan IPS pada Server

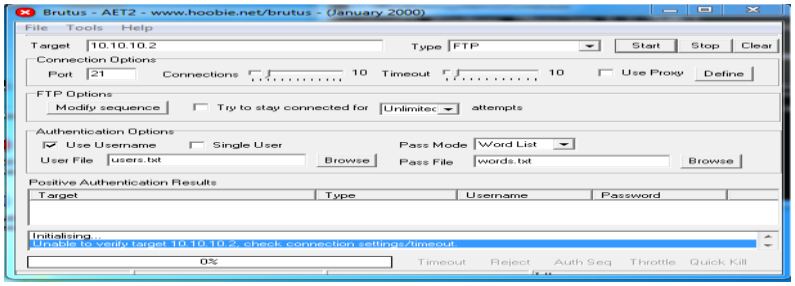
IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada *Server Mikrotik*. Dalam penelitian ini dilakukan uji coba penyerangan yaitu *bruteforce*, berikut adalah hasil uji coba dalam penelitian ini :

Gambar 2. Serangan *Bruteforce* dengan Brutus Berhasil Dicegah

Gambar 2 adalah proses serangan bruteforce yang dilakukan dengan menggunakan aplikasi brutus. Dalam proses penyusupan dan pembacaan *username* dan *password*, *IPS* telah mampu mencegah serangan yang terjadi dan dapat terlihat bahwa muncul pesan "*Unable to verifity* 10.10.10.2, *check connection setting/time out*" yang menyatakan bahwa *intruder* mengalami timeout.

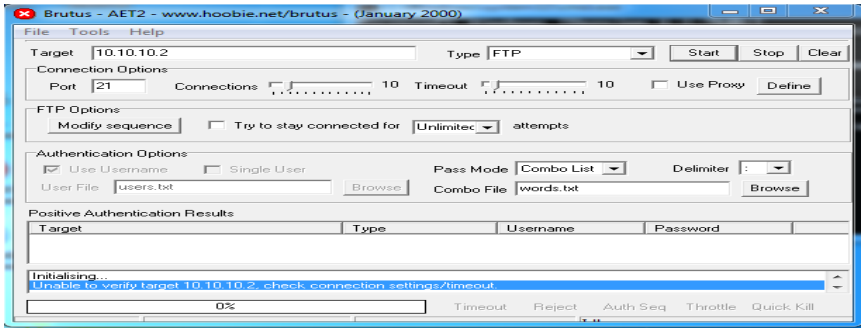
Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada Server Mikrotik. Dalam penelitian ini dilakukan uji coba penyerangan yaitu *bruteforce*dengan *pass mode = word list*, berikut adalah hasil uji coba dalam penelitian ini :



Gambar 3. Serangan *Bruteforce Pass Mode = Word List* dengan Brutus Berhasil Dicegah

Gambar 3 adalah proses serangan *bruteforce* dengan *pass mode = word list* yang dilakukan dengan menggunakan aplikasi brutus. Dalam proses penyusupan dan pembacaan username dan password, *IPS* telah mampu mencegah serangan yang terjadi dan dapat terlihat bahwa muncul pesan "*Unable to verifity* 10.10.10.2, *check connection setting/time out*" yang menyatakan bahwa intruder mengalami *timeout*.

Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada Server Mikrotik. Dalam penelitian ini dilakukan uji coba penyerangan yaitu *bruteforce*dengan *pass mode = combo list*, berikut adalah hasil uji coba dalam penelitian ini

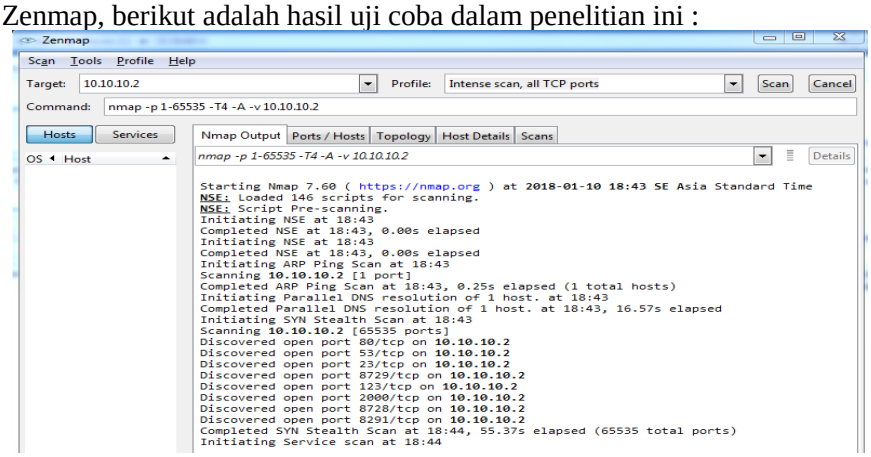


IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Gambar 4. Serangan *Bruteforce Pass Mode = Combo List* dengan Brutus Berhasil Dicegah

Gambar 4 adalah proses serangan bruteforce dengan *pass mode = combo list* yang dilakukan dengan menggunakan aplikasi brutus. Dalam proses penyusupan dan pembacaan username dan password, *IPS* telah mampu mencegah serangan yang terjadi dan dapat terlihat bahwa muncul pesan "*Unable to verifity* 10.10.10.2, *check connection setting/time out*" yang menyatakan bahwa intruder mengalami timeout.

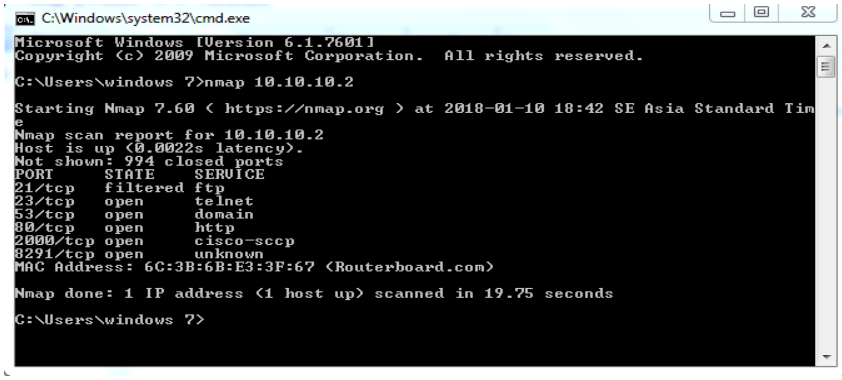
Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada Server Mikrotik. Dalam penelitian ini dilakukan uji coba penyerangan yaitu*port scanning* dengan Zenmap, berikut adalah hasil uji coba dalam penelitian ini :



Gambar 5. Serangan *Port Scanning*dengan Nmap Berhasil Dicegah

Serangan *PortScanning* menggunakan *zenmap* pada *client* 1 dengan *IP* target 10.10.10.2, pada Gambar 5 memperlihatkan bahwa *client* 1 telah melakukan *portscanning* namun tidak bisa mendeteksi *port*21 karena telah diterapkan *IPS* pada server mikrotik.

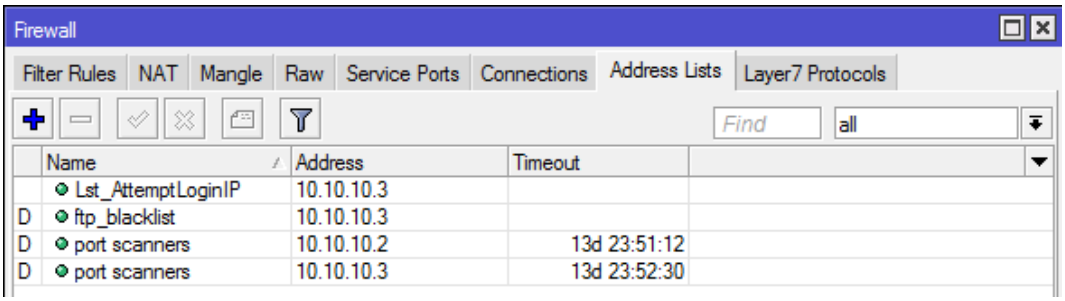
Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada Server Mikrotik. Dalam penelitian ini dilakukan uji coba penyerangan yaitu*port scanning* dengan Nmap pada *windows* 7, berikut adalah hasil uji coba dalam penelitian ini :



Gambar 6. Serangan *Port Scanning* dengan Nmap pada windows 7 berhasil dicegah

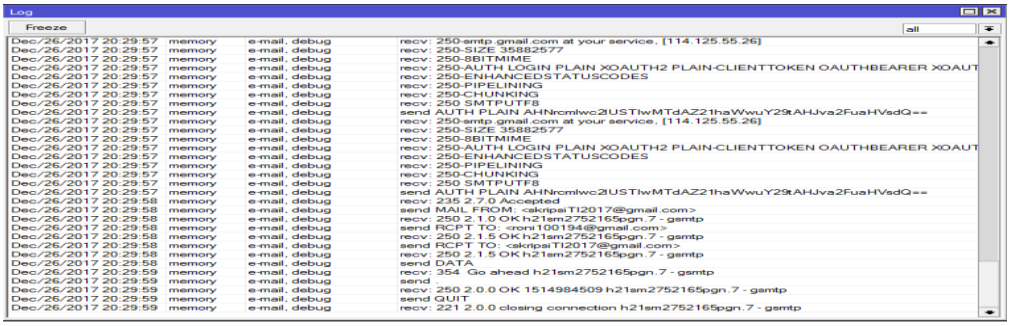
Serangan *PortScanning* menggunakan *zenmap* pada *client* 1 dengan IP target 10.10.10.2, pada Gambar 6 memperlihatkan bahwa *client* 1 telah melakukan *portscanning* dan berhasil dicegah oleh *IPS* pada server mikrotik.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346



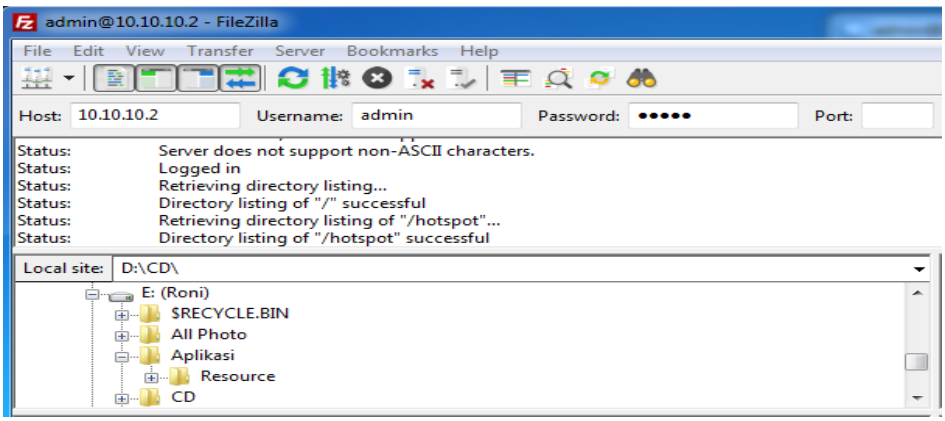
Gambar 7. Tampilan *Address List* Pada *Firewall*

Berikut adalah tampilan *log* mikrotik setelah penerapan *IPS* :



Gambar 8. Tampilan *Log* Mikrotik Setelah Penerapan *IPS*

Pada gambar 8 memperlihatkan log aktivitas yang terjadi dimana pada tanggal 26 Desember 2017 sudah tidak terjadi *login failure for user* admin *from* 10.10.10.3 via ftp. Berikut adalah tampilan filezilla dengan host 10.10.10.2, *username* admin dan *password* admin.



Gambar 9. Tampilan *Server FTPFilezilla*

Gambar 9 menunjukkan tampilan filezilla setelah connect ke host dan dapat dilihat directori E. Berikut adalah tabel perbandingan yang menjelaskan kondisi sebelum dan setelah penerapan *IPS* pada router mikrotik.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

Tabel 1. Perbandingan Sebelum dan Setelah Penerapan *IPS*

Action	Sebelum Menerapkan IPS		Setelah Menerapkan IPS	
Nama Aplikasi Penyerang	Zenmap	Brutus	Zenmap	Brutus
Jenis Serangan	Port Scanning	Bruteforce	Port Scanning	Bruteforce
Hasil Serangan	Port 21 Open	Get Username = Admin Get Password = Admin	Port 21 Filtered	Connection Timeout
Tampilan Log Mikrotik	—	Login Failure	—	—
Email Pemberitahuan Serangan	—	Send To SkripsiTi2018@gmail.com	—	—

Tabel 1 menjelaskan bahwa poin yang dibandingkan yaitu nama aplikasi penyerang, jenis serangan, hasil serangan, tampilan *log* mikrotik dan *email* pemberitahuan serangan.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan dalam penelitian yang Berjudul Simulasi Implementasi *Intrusion Prevention system* Pada Router Mikrotik maka dapat disimpulkan sebagai berikut :

1. Serangan atau penyusupan dapat dicegah dengan menerapkan *Intusion Prevention System(IPS).*
2. Serangan terdeteksi tergantung pada pola serangan yang ada didalam *ruleIPS* tersebut. Untuk itu pengelolaan *filter rules*pada perangkat *IPS* harus secara rutin melakukan pengembangan *rules.*
3. Serangan yang dilakukan dengan software brutus dalam bentuk *bruteforce* sudah bisa dicegah secara maksimal.
4. Serangan yang dilakukan dengan Nmap pada command prompt *windows* 7 dalam bentuk *port scanning*masih belum bisa dicegah secara maksimal karena *IPS* masih membutuhkan beberapa kali serangan untuk bisa mendeteksi serangan dari *ip* yang sama.
5. *Log* mikrotik bekerja dengan maksimal untuk mendeteksi serangan yang terjadi.

5. SARAN

Dari pembahasan serta pengujian yang dilakukan tentunya terdapat hasil dan kendala selama proses pengerjaan maupun dari hasil yang diperoleh. Ada beberapa hal yang perlu dipertimbangkan untuk proses pengembangan selanjutnya yaitu:

1. Untuk pengembangan selanjutnya sebaiknya menggunakan lebih banyak aplikasi penyerangan agar *rulesIPS* yang diterapkan bisa bekerja lebih maksimal.
2. Sebaiknya menggunakan *router board* dengan versi yang lebih tinggi agar bekerja maksimal pada jaringan yang lebih luas.
3. Sebaiknya menambah rules serangan agar tidak hanya terbatas pada serangan *bruterforce*, contohnya *rules* serangan *Dos*.

IT Journal Research and Development
Vol.3, No.1, Agustus 2018 e-ISSN: 2528-4053
DOI : 10.25299/itjrd.2018.vol3(1).1346

DAFTAR PUSTAKA

[1] Y. Arta, E. A. Kadir and D. Suryani, "KNOPPIX: Parallel computer design and results comparison speed analysis used AMDAHL theory," *2016 4th International Conference on Information and Communication Technology (ICoICT)*, Bandung, 2016, pp. 1-5. doi: 10.1109/ICoICT.2016.7571947

[2] Arta, Y. (2017). Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal. *Information Technology Journal Research And Development*, *2*(1), 43-50.

[3] Novendra, Y., Arta, Y., & Siswanto, A. (2018). Analisis Perbandingan Kinerja Routing OSPF Dan EIGRP. *Information Technology Journal Research And Development*, *2*(2), 97-106.

[4] Arta, Y. (2017). Penerapan Metode Round Robin Pada Jaringan Multihoming Di Computer Cluster. *Information Technology Journal Research And Development*, *1*(2), 26-35.

[5] Ariyus, Doni., 2006, *Internet Firewall*, Graha Ilmu, Yogyakarta

[6] Arifin, Zainal., 2005, Langkah Mudah Membangun Jaringan Komputer, Andi, Yogyakarta

[7] Nurmiati, Evy., 2012, Analisi dan Perancangan Web Server Pada Handphone Vol.5, No.2

[8] Affandi, Mohammad., Setyowibowo Sigit., 2013, Impelementasi *Snort* Sebagai Alat Pendeteksi Intrusi Menggunakan Linux Vol.4, No.2

[9] Kurniawan, Adhitya., Putri, Nabilla, Sayyidah., Hermanto, Dedy., 2016, Impelementasi *Intrusion Prevention System (IPS)* Menggunakan *Snort*, IP *Tables*, dan *Honeypot* pada Router Mikrotik.

[10] Towidjojo, Rendra., 2016, Mikrotik Kungfu, Jasakom.com

[11] Suhartono, Didit., Riyanto, Dwi, Andi., Astomo, Widy, Yogi., 2015., *Intrusion Detection Prevention System (IDPS)* Pada *Local Area Network (LAN)* Vol.8, No.1

[12] Ariyadi, Tamsir., Kunang, Novaria, Yesi., Santi Rusmala., 2012., Impelementasi *Intrusion Prevention System (IPS)* Pada Jaringan Komputer Kampus B Universitas Bina Darma

[13] Syafrizal, Melwin., 2017, 7 *Layer Osi*, Yogyakarta

[14] Yugianto, Gin-Gin, Rachman, Oscar., 2012, Router Teknologi, Konsep, Konfigurasi, dan Troubleshooting, INFORMATIKA, Bandung

[15] Syukur, A. (2018). Analisis Management Bandwidth Menggunakan Metode Per Connection Queue (PCQ) dengan Authentikasi RADIUS. *IT Journal Research And Development, 2*(2), 78 - 89.